Claims 1-14, 16, 17, 19, and 20 are pending.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/16/2010 has been entered.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an in person interview with SID NERAYAN and EBENESAR THOMAS on 6/2/2010.

The application has been amended as follows:

Claim 5 – line 1: Change Claim 1 with Claim 3.

Allowable Subject Matter

Claims 1-14, 16, 17, 19, and 20 are allowed.

The following is an examiner's statement of reasons for allowance:

The prior art fails to disclose a coefficient table providing first to fourth coefficients in response to said row index. Van Buer discloses a bit-wise exclusive or between a round key and data before providing the output of the x-or operation for substitution. The operation of Van Buer appears to be more of a mix operation as opposed to the claimed invention which provides for the inputs based on row and column indexes (See Fig. 7 of the instant application). The prior art further fails to disclose the first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substation value with the first to fourth coefficients. The x-or of Van Buer cannot correspond to a multiplication function as disclosed by the claimed invention. Van Buer discloses that each octet W1, W2, W3, and W4 is transformed by, respectively, operations x2 and x3 in GF. More specifically, Van Buer discloses a mixing logic where the multiplication of each octet W1, W2, W3, and W4 with the operations x2 and x3 is performed before providing a value to the S-box (See Fig. 13 of Van Buer). The claimed invention discloses this multiplication takes place after values are received from the s-box.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Randal D. Moran/
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435